

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

JUSTIN DONNELL and A.D. and T.D.,
minors, by their parent JUSTIN
DONNELL, *individually, and on behalf of
all others similarly situated,*

Plaintiffs,

v.

VTECH ELECTRONICS NORTH
AMERICA, L.L.C. and VTECH
HOLDINGS LIMITED,

Defendants.

CASE NO: 1:15-cv-11280

COMPLAINT (CLASS ACTION)

JURY TRIAL DEMANDED

1. Defendants (collectively, “VTech”) are the leading manufacturer and distributor of digital learning toys. Their products allow children to browse the Internet and communicate with each other. Parents can also download educational content for their children, including learning games and e-books.

2. Children share a significant amount of personal information when they use VTech’s products, including their photographs, names, gender, and date of birth. Their parents also share private information including their names, e-mail addresses, passwords, IP addresses, and home addresses. VTech tells its customers that providing this information to the company is

required so that it can “identify the customer, market [its] content and track [customer] downloads.”¹

3. The information VTech requires from its users links parents to their children—this means, among other things, that VTech has a child’s physical address linked to his or her picture and name. Given the highly sensitive nature of the information VTech requires from its customers, keeping this information secure and private is necessary to ensure each child’s safety.

4. Reasonable parents would never knowingly purchase a product or service that would compromise their child’s safety by exposing the child’s picture, name, date of birth, and address to the world. Indeed, VTech at all times represented that it kept its data secure. Despite these representations, VTech failed to take reasonable security precautions. Its product was vulnerable to what is known as a Structured Query Language (“SQL”) “injection attack,” which security experts explain exploits “*the very first type of flaw that should be eliminated from any Web application.*”²

5. Because VTech’s security was inadequate, on November 14, 2015, hackers obtained personal information from more than 2.8 million children in the United States, as well as their parents.³ VTech confirmed and admitted that an “unauthorized party accessed VTech customer data.”⁴ In a statement released a few days later, VTech stated that the database

¹ FAQ about Data Breach on VTech Learning Lodge (last updated: 16:30, December 11, 2015, HKT), https://www.vtech.com/en/press_release/2015/faq-about-data-breach-on-vtech-learning-lodge/#11.

² Matthew J. Schwartz, Why VTech Breach is So Bad—and So Avoidable, *Bank Info Security* (Dec. 3, 2015), <http://www.bankinfosecurity.com/vtech-breach-so-bad-so-avoidable-a-8721/op-1>

³ Jeremy Kirk, Toy maker VTech says breach hit 6.4 million kids’ accounts, *Computerworld* (Dec. 1, 2015), <http://www.computerworld.com/article/3011166/security/toy-maker-vtech-says-breach-hit-64-million-kids-accounts.html>.

⁴ Data Breach on VTech Learning Lodge (Nov. 27, 2015), https://www.vtech.com/en/press_release/2015/statement/

contained profile information including names, email addresses, download history, passwords and mailing addresses.⁵ The database also included information on young children, including their names, genders and birthdates.⁶

6. Specifically, on December 3, 2015, VTech purportedly disclosed the extent of the data breach on their web site. The following types of personal information were compromised in the breach:

- Parent account information including name, email address, secret question and answer for password retrieval, IP address, mailing address, download history and encrypted password.
- Kid profiles include name, genders and birthdates.
- Encrypted Learning Lodge's contents, including Kid Connect's profile photos, undelivered Kid Connect messages, bulletin board postings and Learning Lodge content (ebooks, apps, games etc.).
- Download sales report logs.⁷

7. A number of security researchers confirmed that this breach happened because VTech's security was poorly designed and implemented.

a. Soon after the breach was disclosed, security expert Troy Hunt explained that VTech's security was poorly designed and implemented. He noted that password could be cracked "in next to no time," and that VTech failed to use even basic encryption to transmit information such as "passwords, parent's details, and [personal identifying information] about kids[.]"⁸

⁵ FAQ about Data Breach, *supra* note 1.

⁶ *Id.*

⁷ FAQ about Data Breach on VTech Learning Lodge (Dec. 3, 2015), https://www.vtech.com/en/press_release/2015/faq-about-data-breach-on-vtech-learning-lodge/

⁸ Troy Hunt, When children are breached—inside the massive VTech hack, TroyHunt.com (Nov. 28, 2015), <http://www.troyhunt.com/2015/11/when-children-are-breached-inside.html>.

b. On November 30, 2015, security expert Lorenzo Franceschi-Bicchierai reported that VTech appeared to have “left thousands of pictures of parents and kids and a year’s worth of chat logs stored online in a way easily accessible to hackers.”⁹

8. Plaintiffs and the proposed class members they seek to represent have suffered damages and will continue to suffer them in the future. Among other things:

a. Purchaser Subclass members paid for one thing (a safe, secure product for their children), but VTech instead sold them a different, much less valuable thing (an insecure product). Indeed, what VTech sold arguably has *no* value at all because no reasonable parent would publically disclose their child’s name, picture, date of birth, and physical address.

b. Class members’ PII is now much less valuable and VTech cannot control how it will be used in the future.

c. Class members’ PII was disclosed without consent.

d. Class members now face costs, including out-of-pocket expenses, associated with the prevention, detection, and recovery from identity theft. There are also lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity data misuse.

⁹ Lorenzo Franceschi-Bicchierai, Hacker Obtained Children’s Headshots and Chatlogs From Toymaker VTech, *Motherboard* (Nov. 30, 2015), <http://motherboard.vice.com/read/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech>.

e. Class members face continued risk to their PII, which remains in VTech's possession and is subject to further breaches so long as VTech fails to undertake appropriate measures to protect the PII in their possession.

9. Mr. Donnell, A.D., and T.D., on behalf of themselves and others similarly situated, seek injunctive relief to compel VTech to implement adequate security, damages to compensate purchasers for the significant personal security costs they must now incur, damages because consumers purchased products that were in reality worth much less than their advertised value, and equitable relief including disgorgement of wrongful profits.

PARTIES

Plaintiff Justin Donnell

10. Plaintiff Justin Donnell is a citizen of the Commonwealth of Pennsylvania, and a resident of Verona, Pennsylvania.

11. Mr. Donnell purchased two of VTech's "InnoTab2S" learning products ("Devices") as Christmas gifts for his two children around November or December 2012. The instructions that accompanied the Devices required that Plaintiff Donnell first download a web-connected program called "The Learning Lodge." The Learning Lodge application and VTech web site required that Mr. Donnell follow a set of procedures to both register and create an account with VTech for himself and then associate the Devices with his VTech account. Mr. Donnell was required to register the Devices with VTech in order for his children use the Devices (e.g., download applications, etc.). Mr. Donnell then registered with VTech, created a log-in name and a password, and then associated each of the Devices with his VTech account. Mr. Donnell then associated each of the Devices with one of his children's names. During the registration process, Mr. Donnell provided personally identifiable information ("PII") to VTech, including, *inter alia*, his full name, and upon information and belief, his address, including zip-

code, and security questions and answers. Mr. Donnell also provided PII of his children, including their names, gender and birthdate.

12. When turned on, the Devices were always connected to the Internet through Mr. Donnell's wireless network. Between December 2012 and November 2015, Mr. Donnell's children used the Devices and shopped for and purchased applications offered for sale by the VTech. During that same time, Mr. Donnell accessed and interacted with the VTech web site by downloading and paying for applications offered for sale by VTech.

13. On November 27, 2015, Mr. Donnell received an email from VTech with the subject line "Important Security Message for your VTech Learning Lodge Account." It informed him that VTech "...discovered an unauthorized party accessed VTech customer data on our Learning Lodge app store customer database on November 14 HKT. Our records show that you are a customer of the Learning Lodge...Our customer database contains general user profile information including name, email address, encrypted password, secret question and answer for password retrieval, IP address, mailing address and download history" ("November 27, 2015 Email"). The November 27, 2015 email was electronically signed by the President of VTech Holdings, King F. Pang.

14. That same day, Mr. Donnell commenced his own investigation to find out the nature and extent to which his family's information had been exposed by VTech. He independently verified that his account with VTech was involved with the breach through an online service.¹⁰ He then undertook various time-consuming steps to attempt to mitigate the damages from VTech's breach, including changing all exposed information on VTech's website

¹⁰ See <https://haveibeenpwned.com/>.

that its system would allow him to change. On information and belief, some of Mr. Donnell's personal information remains accessible from VTech's web site.

15. Mr. Donnell has attempted to delete his VTech account in its entirety, including all the information contained therein, but VTech's website will not allow him to delete his account. Indeed, when Mr. Donnell contacted VTech through its website to inquire how to delete his account, he received a response on or about December 4, 2015 that "...there is no option for users to delete their accounts." For this reason, upon information and belief, Mr. Donnell's account remains active.

Plaintiff A.D., by her Parent, Justin Donnell

16. Plaintiff A.D. is a minor child, a citizen of the Commonwealth of Pennsylvania, and a resident of Verona, Pennsylvania.

17. Plaintiff A.D.'s sensitive and personal data—including her name, birthdate, photograph, and gender—was compromised because VTech allowed it to be exposed.

Plaintiff T.D., by his Parent, Justin Donnell

18. Plaintiff T.D. is a minor child, a citizen of the Commonwealth of Pennsylvania, and a resident of Verona, Pennsylvania.

19. Plaintiff T.D.'s sensitive and personal data—including his name, birthdate, photograph, and gender—was compromised because VTech allowed it to be exposed.

Defendant VTech Holdings Limited

20. Defendant VTech Holdings Limited is a Chinese company with its headquarters located at 23/F, Tai Ping Industrial Centre, Block 1, 57 Ting Kok Road, Tai Po, New Territories, Hong Kong. It reports revenues of approximately two billion dollars a year, and one of its largest markets is the United States.

21. VTech Holdings manufactures the products at issue in this case for sale in the United States, as indicated by the fact that it has shipped approximately one million of its products to the United States. VTech Holdings takes responsibility for the safety and security of VTech products.¹¹

Defendant VTech Electronics North America, L.L.C.

22. Defendant VTech Electronics North America, L.L.C. is a limited liability company organized under Illinois law with its headquarters located at 1156 West Shure Drive, Suite 200, Arlington Heights, Illinois 60004. It distributes the VTech Holdings products throughout the United States.

JURISDICTION AND VENUE

23. Subject matter jurisdiction is proper because this case has been brought as a class action, the aggregate claims of the proposed class exceeds \$5 million exclusive of interest and costs, the proposed class includes more than 100 members, and one or more of the members of the proposed class resides in a state that is different from a state in which at least one of the Defendants resides. *See* 28 U.S.C. § 1332(d)(2)(A & C).

24. Personal jurisdiction is proper over VTech Holdings because it manufactured the products that are the subject of this litigation for sale in this District and because it caused significant injuries in this District based on the conduct at issue in this litigation. Personal jurisdiction is proper over VTech Electronics because it resides in this District and regularly

¹¹ Richard Adhikari, VTech Hires Mandiant to Shore Up Security for Kids, *Commerce Times* (Dec. 4, 2015), <http://www.ecommercetimes.com/story/82833.html> (indicating that after the breach, VTech Limited hired a security firm to improve its data security).

conducts business here. Personal jurisdiction is also proper because the contract between the parties provides that the exclusive jurisdiction for any dispute is within the District.¹²

25. Venue is proper because at least one defendant is located and transacts business in this District, a substantial portion of the events and conduct giving rise to the violations complained of in this action occurred in this District, and a substantial portion of the injury from Defendants' conduct occurred in this District. Because VTech Electronics North America, L.L.C.'s headquarters is in this District, efficiencies can be gained by litigating this case here, as documents and evidence—including individuals who may be able to provide deposition testimony—are located within this District. *See* 28 U.S.C. §1391(b)(1&2). Venue is also proper because the contract between the parties provides that the exclusive venue for any dispute is within the District.¹³

CHOICE OF LAW

26. The relevant contract between the parties contains an exclusive choice of law clause selecting Illinois law.¹⁴ Illinois law applies to all claims for this reason.

CLASS ACTION ALLEGATIONS

27. Plaintiffs bring this action on behalf of a class of:

All United States residents whose names appear in
VTech's Learning Log Database.

They also bring this action on behalf of the following subclasses

- (A) All adult class members who purchased a VTech product and provided their PII to VTech (the "Purchaser Subclass").
- (B) All minor class members who provided their PII to VTech (the "Minor Subclass").

¹² VTech Privacy Policy, http://www.vtechkids.com/privacy_policy/ (last accessed Dec. 12, 2015).

¹³ *Id.*

¹⁴ *Id.*

Plaintiffs reserve the right to propose these or other subclasses (such as state-wide subclasses) prior to trial to address any manageability concerns the Court may have.

28. Excluded from the proposed class and any subclass are Defendants, their parents, subsidiaries, agents, officers, and directors. Also excluded is any judicial officer assigned to this case and members of his or her staff.

29. Plaintiffs seek class certification under Rule 23(b)(2) and Rule 23(b)(3) of the Federal Rules of Civil Procedure. In the alternative, they seeks class certification under Rule 23(c)(4) because the below common questions predominate as to particular issues that could substantially advance the litigation. The proposed class meets all express and implied requirements of these rules.

30. **Ascertainability.** The class is readily ascertainable because it is objectively defined and meets the ascertainability standard of this Circuit. Indeed, the class consists of individuals whose information appears in VTech's own database and thus meets the ascertainability standard of every Circuit.

31. **Numerosity—Rule 23(a)(1).** VTech admits that the personal information of millions of children and their parents has been compromised. Accordingly, the members of the class are so numerous that joinder of all members is impracticable. On information and belief, Plaintiffs expect discovery to reveal that the number of class members in any given state, including Illinois, would be so numerous that joinder of all members is impracticable.

32. **Commonality—Rule 23(a)(2).** The answer to at least one question common to the class will drive the resolution of this litigation. For example:

a. Whether VTech's product was defective as sold.

- b. Whether VTech's database was defective in that VTech failed to implement basic security measures to keep PII secure.
- c. Whether VTech had a duty to take reasonable and prudent security measures.
- d. Whether VTech failed to take reasonable and prudent security measures.
- e. Whether VTech's failure to take reasonable and prudent security measures caused injury.
- f. Whether VTech disclosed Plaintiffs' and proposed class members' PII without their prior written consent.
- g. Whether Plaintiffs and proposed class members are entitled to damages, declaratory, or injunctive relief.

33. **Typicality—Rule 23(a)(3).** Plaintiffs bring claims for the same type of injury under the same legal theory as the rest of the class. Among other things, all VTech exposed all class members' personal information.

34. **Adequacy—Rule 23(a)(4).** Plaintiffs and their counsel are adequate because: (1) there no conflict between the proposed class representative and other class members, or, to the extent any conflicts develop, undersigned counsel will propose the appointment of interim class counsel to represent the various class members' interests; and (2) that the proposed class representatives and their counsel will vigorously pursue the claims of the class. Plaintiffs have no interests contrary to, or in conflict with, the interests of class members.

35. **Predominance & Superiority—Rule 23(b)(3).** Common issues in this litigation predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. A

class action, moreover, is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

36. **Final injunctive relief is appropriate respecting the class as a whole—Rule 23(b)(2).** Injunctive relief is appropriate because, among other reasons, VTech’s inadequate security exposes all proposed class members to a substantial risk of immediate harm. Injunctive relief is necessary to uniformly protect the proposed class members’ data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (815 ILCS §§ 505/1, *et seq.*) Plaintiffs, individually, and on behalf of the Class

37. Plaintiffs incorporate the above allegations as if fully set forth herein.

38. The Illinois Consumer Fraud and Deceptive Business Practices Act (“ICFA”) (815 ILCS §§ 505/1, *et seq.*) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

39. The ICFA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

40. The ICFA applies to Defendants’ actions and conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

41. Defendants are each a “person” as defined under section 505/1(c) of the ICFA.

42. Plaintiffs and each proposed class member are a “consumer” as defined under section 505/1(e) of the ICFA.

43. Defendants’ tablets and similar devices are “merchandise” within the meaning of section 505/1(b) and the sale of their tablets is considered “trade” or “commerce” under the ICFA.

44. Defendants violated the ICFA by materially misrepresenting facts about their tablets and by omitting material facts about their tablets.

45. Defendants publicly represented that their products and database would keep information that they required Class Members to provide secure, when, in fact, they failed to use even the most basic encryption available to keep that information safe. On their website, Defendants represents that they holds their products and services up to the highest safety standards. Defendant VTech Holding, Ltd.’s Vice Chairman Allen Wong says:

Since the birth of our first electronic learning product in 1980, VTech has been committed to bringing safe and quality learning toys to children. We would like to reaffirm this commitment and assure you that VTech’s products comply with the highest levels of US and European safety standards. Through rigorous testing, we maintain strict control and supervision over the quality of our products to ensure we provide the “Fun and Learning” toys that you have grown to know and trust.¹⁵

46. Despite Defendants’ representations, their products and services did not live up to the highest levels of US safety standards. It is well-recognized that services that use the Internet to transmit and store information in databases should be protected from SQL injection attacks, and in fact can be protected from such attacks via certain defenses and protocols—either in the network, or in the applications, themselves.

¹⁵ A Message from VTech Vice Chairman, Allen Wong, <http://www.vtechkids.com/support/safety> (last accessed Dec. 12, 2015).

47. Had Defendants undertaken the “rigorous testing” they claims to have performed, they would have discovered the security vulnerabilities in their products and services.

48. Defendants knew or should have known that their database and data repositories were vulnerable to unauthorized access by third parties. Despite having this knowledge, Defendants represented that their products and services were safe, and intended that consumers rely upon their representations and purchase Defendants’ products and services.

49. Whether or not Defendants’ products and services were secure and had the potential to or would expose user data is a material consideration for users of Defendants’ products.

50. Consumers were or would have been reasonable in relying upon Defendants’ representations concerning the safety of their products and services, and no reasonable parents would have purchased Defendants’ products or allowed their children to use Defendants’ products if they knew that their data and their children’s data would be exposed.

51. Even if Defendants had never represented that they would keep information safe, however, Defendants would still be liable for fraud. This is so because Defendants concealed that they were not keeping information safe and all reasonable consumers would consider that information material.

52. Defendants concealed and failed to disclose that they:

- Stored passwords as simple, “unsalted” hashes;
- Used an extremely vulnerable hashing algorithm to protect passwords;
- Stored secret questions for password and account recovery in plaintext;
- Linked children’s accounts to home address and other identifying information;
- Failed to use encryption for the transmission of collected data (i.e., no SSL);

- Failed to adequately encrypt stored data;
- Failed to protect against SQL injection;
- Stored customer data in an Internet-accessible database;
- Shared and transmitted collected customer data with an unauthorized party;
- and
- Failed to implement basic user authentication (e.g., by limiting who can gain “root” access).

53. Defendants knew that they were not implementing basic security protections as outlined above. In spite of their failure to implement well-recognized basic security protections, Defendants represented that their products and database would safely store Class Members’ data.

54. Had Defendants not engaged in the fraudulent statements or deceptive omission of material facts described above, Plaintiffs and the members of the Purchaser Subclass would have been presented with an informed choice as to whether or not to buy the tablets, and would have also been presented with the disclosure of information necessary to modify their use of (and their children’s use of) the tablets to avoid a breach of their privacy.

55. Defendants’ material misrepresentations and omissions to Plaintiffs were unfair, deceptive, and fraudulent. No reasonable consumer would have purchased Defendants’ product absent the fraud.

56. Plaintiffs were damaged by Defendants’ conduct directed towards consumers. Defendants misrepresented the safety of their products and database and chose not to disclose that their tablets and the services were not secure because Defendants wanted to create demand for and to sell the tablets. Had VTech disclosed their true security practices (or lack thereof), Plaintiffs would never have purchased VTech’s products or would have paid substantially less

for them (i.e., the value of tablets without adequate security protections is, at a minimum, substantially less than the value of tablets with adequate protection).

57. As a direct and proximate result of Defendants' fraud, Plaintiffs suffered harm in, among other things, the money paid for VTech's products.

SECOND CAUSE OF ACTION
Breach of Contract
Mr. Donnell, individually, and on behalf of the Purchaser Subclass

58. Plaintiffs incorporate the above allegations as if fully set forth herein.

59. In order to obtain an account to use Defendants' services, Defendants required Plaintiffs to complete an online registration process. As part of that process, Defendants required Plaintiffs read and agree to Defendants' Terms and Conditions and Privacy Statement ("TOS"). Contained within the TOS were Defendants' representations regarding privacy and data security.

60. Plaintiff Donnell, like all proposed subclass members, assented to the Terms and Conditions set forth in the TOS.

61. The TOS is a valid and enforceable contract.

62. Plaintiffs' contract was for Defendants' products and services, which included security protections for PII. As part of this contract, Defendants were obligated to implement industry standard security policies and processes to adequately protect Plaintiffs' and the class members' PII. Had Defendants disclosed that their security was inadequate, no reasonable person would have agreed to the contract.

63. Mr. Donnell and the other proposed class members performed under the contract by, among other things registering with Defendants and agreeing to abide by Defendants' TOS.

64. Defendants breached a material term of the contract when they failed to protect Plaintiffs' PII.

65. Defendants provided a materially less valuable product than promised when it failed to protect Plaintiffs' PII.

66. Plaintiffs suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

THIRD CAUSE OF ACTION

Breach of contract—breach of the covenant of good faith and fair dealing Mr. Donnell, individually, and on behalf of the Purchaser Subclass

67. Plaintiffs incorporate the above allegations as if fully set forth herein.

68. To the extent that the express terms of the contract between the parties could be construed to allow Defendants the discretion to provide a product with inadequate security, the implied covenant of good faith and fair dealing nevertheless obligated Defendants to offer a safe and secure product.

69. Plaintiffs suffered actual damages, including an amount equal to the difference in the free-market value of the secure products and services they paid for and the insecure products and services they received.

FOURTH CAUSE OF ACTION

Breach of contract—breach of the implied warranty of merchantability (U.C.C. § 2-314) Mr. Donnell, individually, and on behalf of the Purchaser Subclass

70. Plaintiffs incorporate the above allegations as if fully set forth herein.

71. Defendants are and were at all relevant times a merchant with respect to the tablets.

72. Defendants were and are in actual or constructive privity with all Plaintiffs and all members of the Purchaser Subclass.

a. Plaintiffs had and continue to have sufficient direct dealings with Defendants and/or its authorized dealers, franchisees, representatives, and agents to

establish any required privity of contract. Defendants authorized dealers, franchisees, representatives, and agents were not intended to be the ultimate consumers of the tablets and have no rights under the warranty agreements provided with the tablets.

b. Privity is not required to assert this claim because Plaintiffs and the Purchaser Subclass members are intended third-party beneficiaries of contracts between Defendants and their dealers, franchisees, representatives, and agents.

c. By extending express written warranties to end-users, Defendants brought themselves into privity with all Plaintiffs and Purchaser Subclass members.

73. At all times relevant hereto, applicable law imposed upon Defendants a duty that the tablets be fit for the ordinary purposes for which the tablets are used and that they pass without objection in the trade under the contract description.

74. Defendants have not validly disclaimed, excluded, or modified the implied warranties or duties described above, and any attempted disclaimer or exclusion of the implied warranties was and is ineffectual.

75. The tablets were defective at the time they left the possession of Defendants, as set forth above. Defendants knew or should have known of this defect at the time Plaintiffs purchased the tablets and at the time Plaintiffs entered a contract with Defendants. Thus, the tablets, when sold and at all times thereafter, were not in merchantable condition or quality because they were not fit for their ordinary intended purpose and they do not pass without objection in the trade under the contract description.

76. Plaintiffs used the tablets in a manner consistent with their intended use and performed each and every duty required under the terms of the warranties, except as may have

been excused or prevented by the conduct of Defendants or by operation of law in light of Defendants' unconscionable conduct.

77. Defendants had actual knowledge of, and received timely notice regarding, the fact that their tablets were not secure and, notwithstanding such notice, failed to offer an effective remedy.

78. Defendants breached the implied warranty of merchantability.

79. As a direct and proximate result of Defendants breach of warranties, Plaintiffs suffered economic damage, including loss attributable to the diminished value of their tablets, loss of use of the tablets, monies spent and to be spent to replace their tablets, and money spent on tablets that cannot fulfill their ordinary and intended purpose.

FIFTH CAUSE OF ACTION
Negligence
Plaintiffs, individually, and on behalf of the Class

80. Plaintiffs incorporate the above allegations as if fully set forth herein.

81. Defendants knew or should have known that their database and data repositories were vulnerable to unauthorized access by third parties.

82. Defendants assumed a duty of care to use reasonable means to implement both a policy and process by which they could prevent such unauthorized access. Further, Defendants were responsible for engaging in supervision, monitoring, and oversight consistent with the PII that was collected, used, and shared by it.

83. Defendants owed a duty of care to Plaintiffs because Defendants stored the class members' PII and they were foreseeable and probable victims of any inadequate security related policies and practices.

84. Defendants breached these duties by failing to take reasonable measures or to implement reasonable policies and procedures to prevent the unauthorized access to the PII of Plaintiffs.

85. As a result of the breach, Plaintiffs suffered damages, and the damages available to the Purchaser Subclass by way of contract remedies would be inadequate to fully compensate them for their losses.

SIXTH CAUSE OF ACTION
Declaratory Relief
Plaintiffs, individually, and on behalf of the Class

86. Plaintiffs incorporate by reference all factual allegations as if fully set forth herein.

87. There is an actual controversy between Defendants and Class Members concerning whether Defendants had a duty to implement recognized safeguards to protect the PII of Plaintiffs and Class Members.

88. Pursuant to 28 U.S.C. § 2201, this Court may “declare the rights and legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought.”

89. Accordingly, Plaintiffs and Class Members seek a declaration that Defendants have a duty to implement safeguards to guard against the future exposure of Plaintiffs’ and Class Members’ PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

- a. Certify this case as a class action, appoint Plaintiffs as Class representatives, and appoint Plaintiffs’ counsel to represent the Class;

- b. Award Plaintiff and Class Members appropriate relief, including actual and statutory damages;
- c. Award equitable, injunctive, and declaratory relief as may be appropriate, including without limitation an injunction;
- d. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;
- e. Award pre-judgment and post-judgment interest as prescribed by law; and
- f. Grant further and additional relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: December 15, 2015

Respectfully submitted,

By: /s/ Edward A. Wallace

Edward A. Wallace
eaw@wexlerwallace.com
Amy E. Keller
aek@wexlerwallace.com
Tyler J. Story
tjs@wexlerwallace.com
WEXLER WALLACE LLP
55 West Monroe Street, Suite 3300
Chicago, Illinois 60603
312.346.2222

Steven W. Teppler
steppler@abbottlawpa.com
ABBOTT LAW GROUP P.A.
2929 Plummer Cove Road
Jacksonville, Florida 32223
904.292.1111

Michael W. Sobol*
msobol@lchb.com
Roger N. Heller

rheller@lchb.com
LIEFF, CABRASER, HEIMANN
& BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
415.956.1000

Jason L. Lichtman
jlichtman@lchb.com
LIEFF, CABRASER, HEIMANN
& BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013
212.355.9500

John A. Yanchunis*
JYanchunis@ForThePeople.com
MORGAN & MORGAN, PA
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
813.223.5505

Gregory F. Coleman
greg@gregcolemanlaw.com
GREG COLEMAN LAW PC
800 South Gay Street
Suite 1100
Knoxville, Tennessee 37929
865.247.0080

Gary E. Mason*
gmason@wbmlp.com
WHITFIELD BRYSON & MASON LLP
1625 Massachusetts Ave. NW 605
Washington, D.C. 20036
202.429.2290

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice applications forthcoming*